

USDC SDNY DOCUMENT ELECTRONICALLY FILED DOC #: _____ DATE FILED: 11/15/2021
--

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----- X
CISCO SYSTEMS, INC.

Plaintiff,

-against-

SYNAMEDIA LTD. F/K/A TRITON UK BIDCO:
LIMITED

Defendant.
----- X

Civ. A. No. 1:20-CV-10879-LTS-SN

ESI PROTOCOL

Plaintiffs Cisco Systems, Inc. (“Cisco”) and Defendant Synamedia Ltd. f/k/a Triton UK Bidco Limited (“Synamedia”) have agreed to the procedures and protocols set forth in this Order shall govern the production of Electronically Stored Information (“ESI”) in this matter.

A. SCOPE

The procedures and protocols set forth in this Agreement shall govern the production of ESI in this matter, unless the Parties agree in writing to change them or they are changed by the Court at the request of a Party. The Parties agree that discovery measures that do not reasonably or meaningfully lead to resolution of the claims and defenses in this matter in the most just, speedy, and inexpensive manner may be avoided. To the extent that third parties may produce documents in this case, the Parties agree to request that such third parties adopt this Agreement.

B. DEFINITIONS

1. “**ESI**” means information that is stored electronically, regardless of the media or whether it is in the original format in which it was created, as opposed to stored in hard copy (i.e., on paper).
2. “**Metadata**” means the generic term used to describe the structural information of a file that contains data *about* the file, as opposed to

describing the content of a file, as per the Sedona Conference's Glossary of Terms. The Parties have initially agreed upon a set of metadata and coding fields to produce, *see infra* Section H.2. The Parties will provide metadata to the extent it was maintained in the ordinary course of business, with the exception of BEGBATES, ENDBATES, BEGATTACH, ENDATTACH, FILE_LINK (for native-produced files only), DOCTYPE, MD5HASH, DATESVD (for non-emails only), and CUSTODIAN, which must be provided for all documents. The Parties agree that production of metadata concerning novel or proprietary file formats may require special arrangements, and the Parties agree to meet and confer regarding any production.

3. **“Native Format”** means and refers to the format of ESI in which it was generated or as it is ordinarily maintained by the Producing Party in the usual course of its business and in its regularly conducted activities.
4. **“Static Image(s)”** means a representation of ESI produced by converting a Native File into a standard image format capable of being viewed and printed on standard computer systems. A Tagged Image File Format (TIFF) image is an example of a Static Image.
5. **“OCR”** means the optical character recognition file which is created by software used in conjunction with a scanner that is capable of reading text-based documents and making such documents searchable using appropriate software.

6. **“Extracted Text”** means the text extracted from a Native File and includes all header, footer and document body information.
7. **“Party”** or **“Parties”** means or refers to the named Plaintiff and/or Defendant in the above-captioned case.
8. **“Search Methods”** means the use of search terms, date range restrictions, data sampling processes, computer assisted review that uses software to evaluate information within documents and determine relevancy based on applicable algorithms, or selection criteria as a means of identifying data reasonably likely to contain relevant information.

C. COOPERATION

The Parties are aware of the importance the Court places on cooperation and commit to cooperate in good faith.

D. LIAISON

The parties have identified liaisons to each other who are and will be knowledgeable about and responsible for discussing their respective ESI. Each e-discovery liaison will be, or have access to those who are, knowledgeable about the technical aspects of e-discovery, including the location, nature, accessibility, format, collection, search methodologies, and production of ESI in this matter. The parties will rely on the liaisons, as needed, to confer about ESI and to help resolve disputes without court intervention.

E. DISPUTES

The Parties shall meet and confer (through telephone, video conference, or an in person face-to-face meeting) in good faith on any issue regarding ESI, as necessary, including any relating to custodians and data sources, that arise under this Agreement or otherwise. In the event the

Parties cannot reach an agreement on a disputed matter, the Parties shall submit the matter to the Court in accordance with the Federal Rules of Civil Procedure, the Local Rules of the United States District Courts for the Southern and Eastern Districts of New York and/or the Individual Practices of Chief Judge Laura Taylor Swain and/or Magistrate Judge Sarah Netburn.

F. PRESERVATION

The parties have discussed their preservation obligations and needs and agree that preservation of potentially relevant ESI will be reasonable and proportionate. To reduce the costs and burdens of preservation and to ensure proper ESI is preserved, the parties agree that:

1. They will take reasonable steps to preserve information and documents (including metadata) that are potentially relevant to this litigation, subject to reasonable limitations, which includes limitations on automatic deletion of temporary data.
2. The parties shall agree to add or remove custodians as reasonably necessary. If the parties cannot reach agreement on the addition or removal of any custodian, they will follow the dispute procedure outlined above;
3. The following data sources, although they could contain relevant information, will generally be considered to be not reasonably accessible because of undue burden or cost, and need not be preserved, searched, reviewed, or produced:
 - i. ESI contained on “Backup systems” (e.g., systems that periodically store electronic data on tape, floppy disk, optical media, or comparable media to permit the recovery of the information in the event of a system failure);

- ii. Voicemails, instant messages, and similar non-email communication;
 - iii. Deleted fragmented or slack data or other data only accessible by forensics;
 - iv. Random access, cache or other ephemeral data;
 - v. On-line data access data such as temporary internet files or cookies;
 - vi. Broken hard drives;
 - vii. Deleted or corrupted files or file fragments that require recovery through forensic measures, or electronic files with unknown file extensions;
 - viii. System data that are typically overwritten in the normal course of business; and
 - ix. Viruses.
4. Notwithstanding Section F.3, the parties shall preserve the data sources identified in Section F.3 pursuant to their respective document retention policies and/or procedures. If specific facts demonstrate a particular need to preserve, search, review, and/or produce ESI listed above in Section F.3, the party requesting such preservation, search, review, or production shall follow the dispute procedure set forth above.
5. Relevant ESI must be preserved, searched, and produced even if it is password protected. Upon request from the Receiving Party, Producing Party shall provide the requested password if reasonably available. If the Producing Party determines in good faith that the Receiving Party's

request(s) for the password(s) becomes too burdensome, then the Producing Party shall follow the dispute procedure set forth above.

6. In the event a party later determines that preservation is or becomes unduly burdensome for some system, set of custodians, or type of documents, the parties agree to meet and confer in good faith regarding the circumstances in an effort to avoid undue burden and expense.

G. PROPORTIONALITY AND SEARCH TERM PROTOCOL

1. **Use of Search Methods.** To ensure proportionality and exclude ESI that is not relevant to the matter, the Parties agree to meet and confer to discuss the process for gathering ESI and use of reasonable Search Methods as a means to identify relevant ESI for review and production, with an expectation that the Parties will reach an agreement on a set of Search Methods against an agreed-upon list of custodians.
 - (i) It is understood that this may likely be an iterative process. Once a protocol for Search Methods has been agreed to and executed, it may likely need to be refined or customized for specific custodians or ESI types. However, the Parties will undertake best efforts to ensure that the first list of Search Methods is as thorough and appropriate as a first list can be. Upon a reasonable request to further expand or limit the use of Search Methods, the Parties will meet and confer and attempt in good faith to reach an agreement. If the Parties cannot reach agreement, any dispute shall be present to the Court in accordance with the Federal Rules of Civil Procedure, the Local

Rules of the United States District Courts for the Southern and Eastern Districts of New York and/or the Individual Practices of Chief Judge Laura Taylor Swain and/or Magistrate Judge Sarah Netburn.

- (ii) In the event that any Party determines in good faith, after attempting to use the agreed Search Methods, that its use of any of those Search Methods is unreasonable burdensome and inefficient, then it shall meet and confer with the Party that propounded the document request to which it is responding. The propounding Party shall negotiate in good faith to modify the agreed Search Methods. In the absence of a mutually acceptable agreement to modify the agreed Search Methods, the responding Party may apply to the Court to modify the terms of this protocol.
- (iii) The fact that one or more search terms is found in a file, document, or other specific ESI does not establish relevance, responsiveness or discoverability.

- 2. **De-duplication of Production.** Prior to production, each producing party shall de-duplicate ESI globally across all custodians. The basis for de-duplication shall be MD5 or SHA1 hash values at the document level. Attachments shall be taken into account for generating hash values for email files based on the parent/child document grouping. The custodians of de-duplicated copies of documents should be included in the database load file

in the CUSTODIAN field or in a duplication-specific field such as DUPE CUSTODIAN.

3. **Excluded File Types.** The Parties agree that the following ESI file types need not be processed, searched, or produced:
 - i. Word temporary files, such as files that include a tilde as the first character of the filename (e.g. “~mydocument.doc”);
 - ii. “Thumb” files created when a directory is opened in “thumbnail view” indicated by a “thumbs.db” filename; and
 - iii. File extensions listed in Appendix A.
 - iv. Non-searchable embedded files, such as Object Linking and Embedding (OLE) files.

H. PRODUCTION

1. **ESI Production Format.**
 - i. All of Cisco’s ESI productions shall be produced in their native format unless redacted. The confidentiality designation of the document shall appear in the document’s production file name or shall be otherwise identified at the time the document is produced, such as on a label provided with the media containing the file. Redacted documents shall be produced as TIFFS. Each TIFF or natively produced document should be named with a unique Bates Number (e.g., CISCO-0001234).
 - ii. All of Synamedia’s ESI productions shall be produced in TIFF format, with the exception of Excel and PowerPoint files, which

shall be produced in their native format unless redacted. Each TIFF or natively produced document should be named with a unique Bates Number (e.g., SYNAMEDIA-0001234).

2. **Metadata Fields and Metadata File.** The Parties are only obligated to provide the following metadata for all ESI produced to the extent such metadata exists. The parties are not obligated to populate manually any of the fields below if such fields cannot be extracted from a document, with the exception of the following, which must be populated by each party for every document: BEGBATES, ENDBATES, BEGATTACH, ENDATTACH, FILE_LINK (for native-produced files only), DOCTYPE, MD5HASH, DATESVD (for non-emails only), CUSTODIAN, and DESIGNATION.

Field Name	Field Description (If a particular field is not applicable to a particular document and is not otherwise required to be populated by the party, the field will be left blank.)
BEGBATES	Beginning production Bates number (not temporary number).
ENDBATES	Ending production Bates number (not temporary number).
BEGATTACH	For Emails and other container files, this is the first production Bates number of the first document in a family, that is, the body of the cover Email or the original container file. If a document is neither parent nor child, this field is left blank.
ENDATTACH	For Emails and other container files, this is the last production Bates number of the last document in a family. If a document is neither parent nor child, this field is left blank.

Field Name	Field Description (If a particular field is not applicable to a particular document and is not otherwise required to be populated by the party, the field will be left blank.)
DOCUMENTDATE	Last Modified Date for loose files and Date Sent for emails; MM/DD/YYYY HH:MM AM/PM
FILE_NAME / TITLE	Original filename or title of the produced document.
NATIVEFILE	Relative file path of the produced native file on the production media.
TEXTLINK	Relative file path of the produced text file on the production media.
CUSTODIAN	Includes the Individual (Custodian) from whom the documents originated and all Individual(s) whose documents de-duplicated out (De-Duped Custodian)
FROM	The name and email address of the sender of the email/document.
TO	All recipients that were included on the “To” line of the email/document.
CC	All recipients that were included on the “CC” line of the email/document.
BCC	All recipients that were included on the “BCC” line of the email/document.
SUBJECT	Subject line of email.

Field Name	Field Description (If a particular field is not applicable to a particular document and is not otherwise required to be populated by the party, the field will be left blank.)
DATECREATED	Date created (format: MM/DD/YYYY).
DATERECEIVED	Date received (format: MM/DD/YYYY).
DATESVD	Original date modified (format: MM/DD/YYYY).
DATESENT	Date email/document was sent (format: MM/DD/YYYY).
DESIGNATION	Confidentiality designation assigned to document.
DOCTYPE	The application that created the file (e.g. “Word Document” or “Excel Spreadsheet”).
AUTHOR	Author.
FILE_EXT	The file extension.
FILE_SIZE	File size of the native file.
FOLDER NAME	Original file path of the document.

Field Name	Field Description (If a particular field is not applicable to a particular document and is not otherwise required to be populated by the party, the field will be left blank.)
LOCATION / PATH	Original file path or file location of the document.
IMPORTANCE	Email priority level if set.
MD5HASH	A calculated value unique to each identical file. This is the file's "fingerprint."
MIME_TYPE	Name of the program that created the document.
PAGES	Number of pages per document (if produced as image).

3. **Use of Natively Produced Documents at a Deposition, Court Hearing, or Trial, or Converted to Paper Format For Other Use.** If a party elects to use a natively produced document as an exhibit at a deposition, court hearing, or trial, or elects to convert the document to a paper format to use for another purpose (e.g., show to a witness, use by a party's outside counsel for prosecution of its case, etc.), the document shall be rendered in such a format that each page or image must be branded with the file name and unique document number identifier, so that each page of the document has a unique identifying number beginning with ".0001." For example, the first two pages of a document labeled natively CISCO-0001234, should be

labeled CISCO-0001234.0001 and CISCO-0001234.0002. The foregoing requirements shall not apply if it is not technologically feasible (e.g., oversized spreadsheet, audio, video).

4. **TIFFs**. Redacted documents (*see supra* Section H.1) shall be produced as black and white TIFFs, as applicable. *See supra* § H.1. Likewise, documents that exist only in hard copy format shall be scanned and produced as TIFFs.

- i. *TIFF Formatting*. Unless excepted below, single page Group IV TIFFs should be provided, at least 300 dots per inch (dpi) for all documents. Each TIFF image shall be named according to a unique corresponding Bates number associated with the document. Each image shall be branded according to the Bates number. Original document orientation should be maintained (i.e., portrait to portrait and landscape to landscape). TIFFs shall show all text and images that would be visible to a user of the hard copy documents. To the extent that a produced TIFF is a color document, if the producing party has reason to believe (such as by, for example, colored highlighted text, notes, or other delineations that would be not visible or obscured in .tiff format), or if a receiving party reasonably asserts in good faith, that the colors are necessary to understand the substance of the document, the producing party will produce the image in color as a JPEG file.
- ii. *Text Files*. A single multi-page text file shall be provided for each document produced in TIFF, and the filename should match its

respective TIFF filename. A commercially acceptable technology for OCR shall be used for all scanned, hard copy documents. Text files will not contain the redacted portions of the documents and OCR text files will be substituted instead of extracted text files for redacted documents.

- iii. *Image Load Files/Data Load Files.* Each TIFF in a production must be referenced in the corresponding image load file. The total number of documents referenced in a production's data load file should match the total number of designated document breaks in the Image Load file(s) in the production. The total number of pages referenced in a production's image load file should match the total number of TIFF files in the production. The total number of documents in a production should match the total number of records in the data load file.
- iv. *Redaction of Information.* If documents are produced containing redacted information, an electronic copy of the original, unredacted data shall be securely preserved in such a manner so as to preserve without modification, alteration or addition the content of such data including any metadata therein. The Producing Party shall have no obligation to produce the original, unredacted data (including any metadata therein) except by agreement of the Parties or Court order.

5. **Proprietary Files.** To the extent a response to discovery requires production of ESI accessible only through proprietary software, the parties shall meet and confer to finalize the appropriate production format.
6. **Production Media.** The Producing Party shall produce documents on readily accessible, computer or electronic media as the Parties may hereafter agree upon, including CD-ROM, DVD, flash drive, external hard drive (with standard PC compatible interface or access to a secure On-Line Repository agreed upon by the Parties) or via secure FTP site. The Producing Party shall accompany all document productions with a transmittal cover letter identifying by Bates number the documents produced.

I. OBJECTIONS TO ESI PRODUCTION.

If either Party objects to producing the requested ESI on the grounds that such information is not reasonably accessible because of undue burden or cost, or because production in the requested format would impose undue burden or cost, the Party shall describe the nature of the objection with reasonable particularity. This notification shall occur promptly. If possible, the notifying party should describe potential alternative sources or production formats. The Parties will meet and confer in an attempt to resolve the objections if necessary.

J. PRIVILEGE LOGS.

Neither Party is required to log privileged or otherwise legally-protected (from production) ESI or any other material dated after July 10, 2020, the date on which Synamedia sent its first letter to Cisco raising the dispute that led to this litigation (the “cut-off date”). In addition, documents

created by or on behalf of outside litigation counsel and communications with outside litigation counsel, regardless of their date, do not need to be included on any privilege log. The parties reserve the right to request a log of the documents excluded under this provision where good cause exists.

K. NO WAIVER OF PRIVILEGE.

If a Producing Party inadvertently or unintentionally produces any document(s) or information the Producing Party determines was entitled to a claim of privilege or protection from discovery (including but not limited to attorney-client privilege, work product doctrine, and other privilege created by federal or state statute or regulation), the Producing Party shall, within twenty-one (21) days of discovering the inadvertent production, give notice to the Receiving Party in writing of the Producing Party's claim of privilege or protection from discovery. The Receiving Party then shall promptly return, sequester, or destroy the specified document(s) or information; must not use or disclose the information until the privilege or protection claim is resolved; must take reasonable steps to retrieve the information if the Receiving Party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The Producing Party must preserve the information until the claim is resolved.

Inadvertent or unintentional production may not be deemed a waiver in whole or in part of the Producing Party's claim of privilege or immunity from discovery either as to specific documents and information disclosed or on the same or related subject matter based on the facts constituting the inadvertent production. This provision is, and shall be construed as, an Order under Rule 502(d) of the Federal Rules of Evidence. Accordingly, as is explicitly set forth in Rule 502(d), a Party's production of documents, whether inadvertent or intentional, is not a waiver of any privilege or protection "in any other federal or state proceeding." Fed. R. Evid. 502(d).

L. MODIFICATION

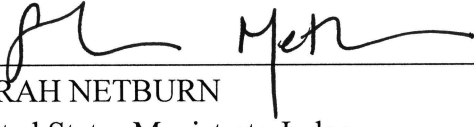
This Stipulated Order may be modified by a Stipulated Order of the parties or by the Court for good cause shown.

Dated: November 10, 2021

Respectfully Submitted,

SO ORDERED.

Dated: November 15, 2021
New York, New York



SARAH NETBURN
United States Magistrate Judge

/s/ Christopher J. Letkewicz

J. Erik Connolly (admitted *pro hac vice*)
Christopher J. Letkewicz (admitted *pro hac vice*)

David S. Almeida

BENESCH, FRIEDLANDER, COPLAN &
ARONOFF LLP

71 South Wacker Drive, Suite 1600

Chicago, Illinois 60606

Telephone: (312) 212-4949

Facsimile: (312) 767-9192

Email: econnolly@beneschlaw.com

cletkewicz@beneschlaw.com

dalmeida@beneschlaw.com

Attorneys for Plaintiff Cisco Systems, Inc.

/s/ Rebecca L. Martin

Matthew D. Parrott

Rebecca L. Martin

FRIED, FRANK, HARRIS, SHRIVER &
JACOBSON LLP

One New York Plaza

New York, New York 10004

Telephone: (212) 859-8000

Facsimile: (212) 859-4000

Email: m.parrott@friedfrank.com

Rebecca.martin@friedfrank.com

*Attorneys for Defendant Synamedia Ltd. f/k/a
Triton UK Bidco Limited*

APPENDIX A**EXCLUDED FILE EXTENSIONS**

EXTENSION	EXCLUDE BECAUSE
\$\$\$	TEMPORARY FILE
286	DEVICE DRIVER
386	DEVICE DRIVER
AFM	ADOBE FONT METRIC
ASP	ACTIVE SERVER PAGE
AVI	MOVIE / ANIMATION
AXF	SOURCE CODE
BACKUP	BACKUP FILE
BAK	BACKUP FILE
BAT	EXECUTABLE
BIN	BINARY DATA
BKF	WINDOWS BACKUP FILE
C	C/C++ SOURCE CODE FILE
CAB	INSTALLER FILE
CFG	BINARY CONFIGURATION FILE
CHM	WINDOWS HELP FILE
CLASS	SOURCE CODE FILE
CMD	COMMAND FILE (TEXT EXECUTABLE)
CNT	WINDOWS HELP CONTENTS TABLE

EXTENSION	EXCLUDE BECAUSE
COM	EXECUTABLE
CONF	SYSTEM OR APPLICATIONS SETTINGS FILE
CONFIG	CONFIGURATION FILE
CPL	CONTROL PANEL APPLET
CS	SOURCE CODE
CSPROJ	SOURCE CODE
CSS	CASCADING STYLE SHEET
CUR	WINDOWS CURSOR
DAT	RAW DATA, PROBABLY BINARY
DATA	RAW DATA, PROBABLY BINARY
DB	DATABASE FILE, PROBABLY BINARY
DBF	DATABASE
DEF	MS VISUAL C++ DEFINITION FILE
DEFAULT	SYSTEM OR APPLICATIONS SETTINGS FILE
DICT	DICTIONARY
DLG	C++ DIALOGUE SCRIPT
DLL	EXECUTABLE
DOT	MS-WORD DOCUMENT TEMPLATE
DS_STORE	COMMERCIAL FILE
DUN	MS DIAL-UP NETWORKING EXPORT
EPS	PRINTER FILE

EXTENSION	EXCLUDE BECAUSE
ERR	SYSTEM FILE
EXE	EXECUTABLE
FON	FONT
FOT	FONT
GAM	GAME
H	SOURCE CODE HEADER/INCLUDE FILE
HLP	HELP FILE
ICO	MS WINDOWS ICON
INF	SETUP INFORMATION FILE
INI	INITIALIZATION FILE
INS	INSTALLSHIELD INSTALL SCRIPT
INX	INSTALLSHIELD INDEX
JAVA	SOURCE CODE
JS	JAVA SCRIPT SOURCE CODE FILE
JSP	JAVA SERVER PAGE
LIB	LIBRARY (EXECUTABLE)
LIVEUPDATE	LIVEUPDATE FILE
LNK	MS WINDOWS SHORTCUT/LINK
LOG	LOG FILE (UNKNOWN SOURCE)
MAK	SOURCE CODE MAKE FILE
MDB	MS ACCESS DATABASE/TEMPLATE/ADDITION

EXTENSION	EXCLUDE BECAUSE
MDE	COMPILED MS ACCESS DATABASE
ME	INFO (E.G. READ.ME), MULTIEDIT CONFIG
MID	AUDIO FILE
MIDI	AUDIO FILE
MP2	AUDIO FILE
MP3	AUDIO FILE
MP4	AUDIO FILE
MSI	MS WINDOWS INSTALLER WIZARD
NLB	ORACLE 7 DATA
O	COMPILER OBJECT
OBJ	COMPILER OBJECT
OCX	OLE CONTROL EXTENSION
OVL	PROGRAM OVERLAY (EXECUTABLE)
PAK	COMPRESSED ARCHIVE, GAME FILE
PDB	MS VISUAL C++ PROGRAM DATABASE (AND OTHER DBS)
PF	MS WINDOWS PREFETCH CACHE
PFB	ADOBE POSTSCRIPT FONT (BINARY)
PFM	ADOBE PRINTER FONT METRICS
PIF	MS WINDOWS PROGRAM INFORMATION
PIP	MS APPLICATION PROFILE SETTINGS
PL	PERL APPLICATION

EXTENSION	EXCLUDE BECAUSE
PNF	PRECOMPILED SETUP INFORMATION
QUE	DATABASE QUERY
QUERY	DATABASE QUERY
README	PROGRAM INFO FILE
RMI	AUDIO FILE
SCR	SCRIPT, SCREEN SAVER,
SQL	DATABASE QUERY
SYM	SYMBOL TABLE
SYS	SYSTEM FILE
SYSLOG	SYSTEM LOG
THEME	MS WINDOWS DESKTOP THEME
TLB	MS WINDOWS OLE TYPE LIBRARY
TMP	TEMPORARY FILE
TTF	TRUE TYPE FONT
UNINSTALL	UNINSTALL FILE
URL	MS WINDOWS INTERNET SHORTCUT
USR	USER INFO FILE
VB	MS VISUAL BASIC.NET SOURCE CODE
VCN	MS VISUAL BASIC.NET SOURCE CODE
VBPROJ	MS VISUAL BASIC.NET PROJECT
VCPROJ	MS VISUAL C++.NET PROJECT

EXTENSION	EXCLUDE BECAUSE
VXD	VIRTUAL DEVICE DRIVER (EXECUTABLE)
WAV	AUDIO FILE